主要内容

七、系统安全

- ◆网络（漏洞）扫描
- ◆DDOS攻击
- ◆APT基本概念和方法

八、无线网络安全（补充）

- ❖移动安全
- ❖WEP协议安全性分析

网络扫描技术

网络扫描技术

- ◆ 背景
  - ❖网络和系统存在漏洞
    - ➢由于网络技术的飞速发展，网络规模迅猛增长和计算机系统日益复杂，导致新的系统漏洞层出不穷
    - ➢由于系统管理员的疏忽或缺乏经验，导致旧有的漏洞依然存在
  - ❖意图：好奇心，入侵前的准备，不停的窥视网上资源
- ◆网络扫描是一种带有入侵性和挑战性的过程
  - ❖ 识别IP地址空间中可访问的主机与服务
  - ❖ 获得网络拓扑结构及其安全机制
  - ❖ 发现、枚举网络中的漏洞与弱点

网络扫描器（scanner）

- ◆扫描器是一把双刃剑，系统管理员使用它来查找系统的潜在漏洞，而黑客利用它进行攻击
  - ❖安全评估的工具：保障系统安全的有效工具
  - ❖网络入侵者收集信息的重要手段
- ◆自动检测远程或本地主机安全性弱点的软件
  - ❖端口扫描器：进行端口探测，检查远程主机上开启的端口
  - ❖漏洞扫描器：把各种安全漏洞集成在一起，自动利用这些安全漏洞对远程主机尝试攻击，从而确定目标主机是否存在这些安全漏洞

漏洞扫描器安装模式

- 漏洞扫描器安装模式有两种：
  - 一种是把漏洞扫描器安装在被扫描的系统中，这种情形适合于单机漏洞扫描
  - 另一种则是把漏洞扫描器安装在一台专用的计算机中，然后通过该计算机来扫描其他系统的漏洞，这种模式适合于扫描网络系统

网络端口扫描

- 目的
  - 了解网络中的详细情况，比如网络拓扑结构，活动主机IP地址
  - 主要扫描服务器，路由器和防火墙
  - 黑客使用扫描工具一般先扫描网关、DMZ系统，各种服务器等Internet周边环境，在控制了网络周边环境后，再继续攻击内部网络
- 分类：
  - 发现活跃主机
  - 跟踪路由

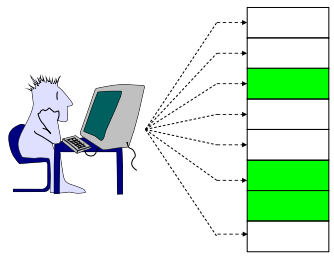
例如：通过超长包探测内部路由器

- 若构造的数据包长度超过目标系统所在路由器的路径最大传输单元（PMTU）且设置禁止分片标志
- 该路由器会反馈ICMP差错报文
  - Fragmentation Needed and Don’t Fragment Bit was Set
  - 从而获取目标系统的**网络拓扑结构**

如何防御网络扫描

- 利用防火墙和路由器的数据包过滤功能来阻塞这些消息
- 阻塞所有流入的ICMP消息
- 过滤从内部网络流出的ICMP超时信
  - 例如，拒绝traceroute的访问

端口扫描技术



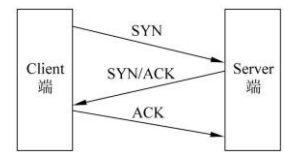
TCP连接知识

- TCP数据包6个标志位
  - URG: 紧急数据包
  - ACK: 确认
  - PSH: 请求急迫操作
  - RST: 连接复位
  - SYN: 连接请求
  - FIN: 结束
- TCP/IP的一些实现原则
  - 当一个SYN或者FIN数据包到达一个关闭的端口，TCP丢弃数据包同时发送一个RST数据包
  - 当一个RST数据包到达一个监听端口，RST被丢弃
  - 当一个RST数据包到达一个关闭的端口，RST被丢弃
  - 当一个包含ACK的数据包到达一个监听端口时，数据包被丢弃，同时发送一个RST数据包
  - 当一个不包含SYN位的数据包到达一个监听端口时，数据包被丢弃
  - 当一个SYN数据包到达一个监听端口时，正常的三阶段握手继续，回答一个SYN|ACK数据包
  - 当一个FIN数据包到达一个监听端口时，数据包被丢弃

TCP connect扫描

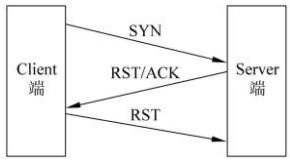
- **最简单的扫描方式，实际上是利用linux提供的系统调用函数connect()与目标主机建立TCP连接，完成三次握手**
- **这种扫描方式会被防火墙记录到访问日志中**
  - **会留下扫描痕迹**
  - **这种扫描不需要有特殊权限**

TCP connect扫描



- **TCP connect端口扫描服务端与客户端建立连接成功（目标端口开放）的过程：**
  - **① Client端发送SYN**
  - **② Server端返回SYN/ACK，表明端口开放**
  - **③ Client端返回ACK，表明连接已建立**
  - **④ Client端主动断开连接**

TCP connect扫描



◆**TCP connect端口扫描服务端与客户端未建立连接成功（目标端口关闭）过程：**

- ❖**① Client端发送SYN**
- ❖**② Server端返回RST/ACK，表明端口关闭**

TCP connect扫描特点

◆实现简单，对操作者的权限没有严格要求

- ❖端口扫描不需要操作者具有root权限

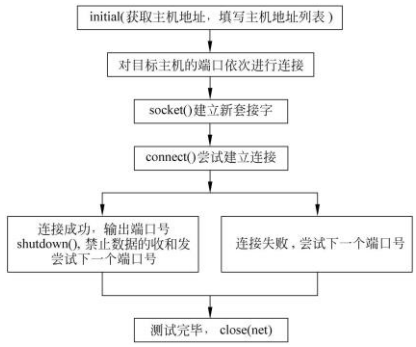
◆扫描速度快

- ❖可以通过并发打开多个套接字，从而加速扫描

◆缺点

- ❖是会在目标主机的日志记录中留下痕迹，易被发现，并且数据包会被过滤掉
- ❖目标主机的logs文件会显示一连串的连接和连接出错的服务信息，并且能很快地使它关闭

TCP connect扫描流程

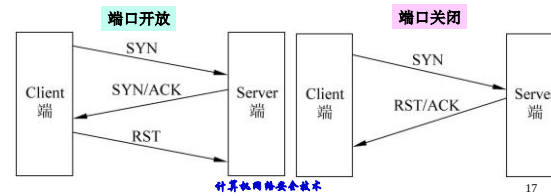


半开放(half open/SYN)扫描

◆**扫描器向目标主机的一个端口发送请求连接的SYN包，扫描器在收到SYN/ACK后，不是发送的ACK应答而是发送RST包请求断开连接**

◆**三次握手就没有完成，未建立正常的TCP连接，因此，这次扫描就不会被记录到系统日志中**

◆**这种扫描技术一般不会在目标主机上留下扫描痕迹。但是，这种扫描需要有root权限**



Nmap扫描器

- **Nmap (Network Mapper) 是一款开放源代码的网络探测和安全审核的工具。**
- **它的设计目标是快速地扫描一个网络或一台主机上的开放的端口**
- **Nmap使用原始IP包来发现网络上有哪些主机**
  - **那些主机提供什么服务(应用程序名和版本)**
  - **那些服务运行在什么操作系统(包括版本信息)**
  - **使用什么类型的包过滤器/防火墙，以及一些其它功能**
- https://nmap.org
- **在Linux、Windows、Mac OS下运行，并且有图形化界面Zenmap**

Nmap的功能

- Nmap包含四项基本功能：
  - 主机发现（Host Discovery）
  - 端口扫描（Port Scanning）
  - 版本侦测（Version Detection）
  - 操作系统侦测（Operating System Detection）
- 在四项基本功能的基础上，Nmap提供防火墙与IDS（Intrusion Detection System,入侵检测系统）的规避技巧，可以综合应用到四个基本功能的各个阶段
- 另外Nmap提供强大的NSE（Nmap Scripting Language）脚本引擎功能，脚本可以对基本功能进行补充和扩展。

Nmap简介

- Nmap输出
  - 扫描目标的列表，以及每个目标的补充信息。
  - “所感兴趣的端口表”是输出信息的关键。表中列出端口号、协议、服务名称和状态
  - 状态可能是open(开放的)、filtered(被过滤的)、closed(关闭的)或者unfiltered(未被过滤的)
- 如果Nmap报告状态组合open|filtered和closed|filtered时
  - 那说明Nmap无法确定该端口处于两个状态中的哪一个状态
- 当要求进行版本探测时，也可以包含软件的版本信息
- 当要求进行IP协议扫描时，Nmap提供所支持的IP协议而不是正在监听的端口的信息
- 除了端口表，Nmap还能提供关于目标主机的进一步信息，包括反向域名、操作系统猜测、设备类型和MAC地址等

Nmap结果

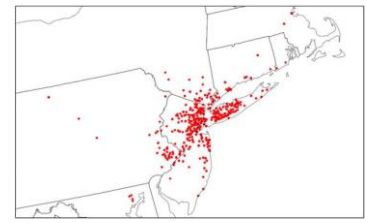
```
C:\>nmap -v 192.168.1.93

Starting Nmap 4.20 ( http://insecure.org ) at 2007-06-28 10:22 中国标准时间
Initiating ARP Ping Scan at 10:22
Scanning 192.168.1.93 [1 port]
Completed ARP Ping Scan at 10:22, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:22
Completed Parallel DNS resolution of 1 host. at 10:22, 13.02s elapsed
Initiating SYN Stealth Scan at 10:22
Scanning 192.168.1.93 [1697 ports]
Discovered open port 21/tcp on 192.168.1.93
Discovered open port 80/tcp on 192.168.1.93
Discovered open port 53/tcp on 192.168.1.93
Discovered open port 443/tcp on 192.168.1.93
Discovered open port 135/tcp on 192.168.1.93
Discovered open port 1025/tcp on 192.168.1.93
Discovered open port 3372/tcp on 192.168.1.93
Discovered open port 1521/tcp on 192.168.1.93
Discovered open port 1031/tcp on 192.168.1.93
Discovered open port 1032/tcp on 192.168.1.93
Discovered open port 1026/tcp on 192.168.1.93
Discovered open port 139/tcp on 192.168.1.93
Discovered open port 445/tcp on 192.168.1.93
Completed SYN Stealth Scan at 10:22, 0.25s elapsed (1697 total ports)
Host 192.168.1.93 appears to be up ... good.
Interesting ports on 192.168.1.93:
Not shown: 1684 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1025/tcp open  NFS-or-IIS
1026/tcp open  LSA-or-nterm
1031/tcp open  iad2
1032/tcp open  iad3
1521/tcp open  oracle
```

ZMap

- 全球互联网包含数十亿个不重复IPv4地址，扫描整个互联网是一项劳动密集型工作，需要耗费几周甚至几个月
- 2013年，密歇根大学研究人员发明扫描攻击Zmap，用一台普通的服务器运行该工具扫描完全球所有互联网地址竟仅用时44分钟！（Nmap需要数周时间）
  - ZMap则是一种“**无状态**”的工具
  - TCP SYN扫描方式
  - 将对方receiver ip地址进行hash，将其处理保存到了sender port和seq number两个字段中，当SYN-ACK回来的时候，就可以根据sender ip、receiver port、ack number这些字段进行校验。
    因此避免了状态存储，接近了网络带宽极限。

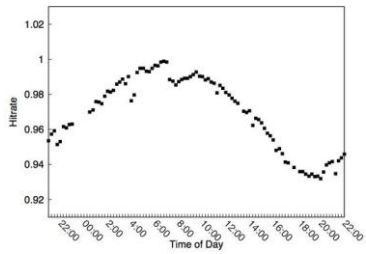
Zmap的实验

- 飓风对互联网的影响
  - 2012年10月29日到31日之间，桑迪飓风（Hurricane Sandy）横扫美国东海岸，密歇根大学的研究团队每隔两个小时就会对整个互联网进行一次扫描。通过将IP地址与地理位置联系起来的方式，研究人员能对哪些地区的网络服务中断情况最为严重进行观察。下面这张地图所显示的就是“收听主机数量减少30%以上的位置”



Zmap的实验

- 互联网的睡眠周期
  - 在一天中的不同时刻进行了整个互联网扫描，然后观察自己能获得多少回复

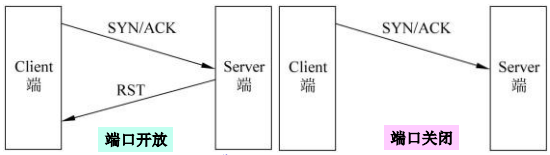


秘密扫描

- 一种不被审计工具所检测的扫描技术
- 通常用于在通过普通的防火墙或路由器的过滤（filtering）时隐藏自己
- 能躲避IDS、防火墙、包过滤器和日志审计，从而获取目标端口的开放或关闭的信息
  - 由于没有包含TCP 三次握手协议的任何部分，所以无法被记录下来，比半连接扫描更为隐蔽
- 缺点是扫描结果的不可靠性会增加，而且扫描主机也需要自己构造IP包
  - 现有的秘密扫描有TCP FIN扫描、TCP ACK扫描、NULL扫描、XMAS扫描和SYN/ACK扫描等

SYN/ACK扫描

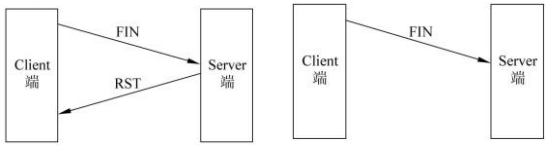
- 这种扫描忽略TCP的三次握手，原来正常的TCP连接可以简化为SYN- SYN /ACK-ACK形式的三次握手来进行
- 扫描主机不向目标主机发送SYN数据包，而发送SYN/ACK数据包
  - 若目标端口开放，目标主机将返回RST信息
  - 若目标端口关闭，目标主机将不返回任何信息，数据包会被丢掉



FIN扫描

- 基于SYN的扫描已经不是一种秘密了，许多防火墙和路由器都有相应的措施，它们会对一些指定的端口进行监视，对这些端口的连接请求全部进行记录
- 许多过滤设备允许FIN数据包通过
  - FIN是中断连接的数据报文，所以许多日志系统不记录这样的数据报文
  - FIN扫描的原理就是向目标主机的某个端口发送一个FIN数据包，该数据包企图关闭一个不曾打开的TCP连接
    - 如果收到RST应答表示这个端口没有开放
    - 反之则端口开放
- 局限性
  - 这种方法和系统的实现有一定的关系
  - 有些操作系统不管端口是否开放，都应答RST
  - 防火墙的存在以及数据包可能在传输过程中丢失，可能无法收到RST，所以这不是一种很有效的扫描方式

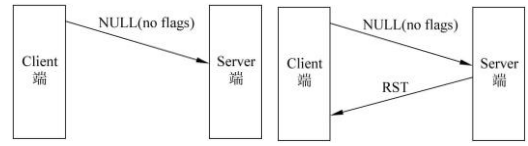
FIN扫描



TCP FIN扫描建立连接成功　　TCP FIN扫描建立连接未成功

- 这种方法可以用来区别操作系统是UNIX还是Windows

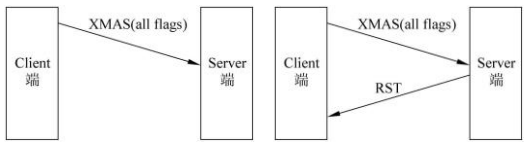
TCP NULL扫描



NULL扫描建立连接成功　　NULL扫描建立连接未成功

- 扫描主机将TCP数据包中的ACK（确认）、FIN（结束连接）、RST（重新设定连接）、SYN（连接同步化要求）、URG（紧急）、PSH(接收端将数据转由应用处理)标志位置空后发送给目标主机
- 根据RFC793，如果目标主机的相应端口是关闭的话，应该发送回一个RST数据包。但实际的系统反映将各不相同。
  - 若目标端口开放，目标主机将不返回任何信息
  - 若目标主机返回RST信息，则表示端口关闭

XMAS扫描



XMAS扫描建立连接成功　　XMAS扫描建立连接未成功

- XMAS扫描原理和NULL扫描的类似，将TCP数据包中的ACK、FIN、RST、SYN、URG、PSH标志位置1后发送给目标主机
  - 在目标端口开放的情况下，目标主机将不返回任何信息
  - 若目标端口关闭，则目标主机将返回RST信息

TCP 扫描说明

- MS Windows、Cisco、BSD、HP/UX、MVS以及IRIX等操作系统如果通过TCP FIN、XMAS以及NULL扫描等方式进行扫描，对于打开的端口也会发送RST数据包，即使所有端口都关闭，也可以进行应答
- 根据制作Nmap的Fyodor的方案，使用FIN、XMAS或者NULL方式进行扫描，如果所有端口都关闭，那么就可以进行TCP SYN扫描
- 如果出现打开的端口，操作系统就会知道是属于MS Windows、Cisco、BSD、HP/UX、MVS以及IRIX中的哪类了

IP碎片扫描

- 以细小的IP碎片包实现SYN，FIN，XMAS或NULL扫描攻击
- 即将TCP包头分别放在几个不同的数据包中，从而躲过包过滤防火墙的检测
- 扫描主机并不是直接发送TCP探测数据包，而是将数据包分成两个较小的IP段
- 这样就将一个TCP头分成好几个数据包，从而过滤器就很难探测到，扫描就可以在不被发现的情况下进行
- 但是需要注意的是，一些程序在处理这些小数据包时会有些麻烦，并且不同的操作系统在处理这个数据包的时候，通常会出现问题

普通UDP扫描

- 这种扫描攻击用来确定目标主机上哪个UDP端口开放
- 通常是通过发送零字节的UDP数据包到目标机器的各个UDP端口
  - 如果收到一个“ICMP端口无法到达”的回应，则该端口是关闭的
  - 否则可以认为它是打开的
- UDP扫描的意义：确定目标主机是否存在那些基于UDP协议的服务如snmp、tftp、NFS、DNS
- 局限性
  - ICMP和UDP不可靠，需要多次扫描
  - RFC对ICMP数据包的产生速率有限制
    - RFC1812的中对ICMP错误报文的生成速度做出了限制。例如Linux就将ICMP报文的生成速度限制为每4秒钟80个，当超出这个限制的时候，还要暂停1/4秒。
  - 需要有管理员权限

UDP recvfrom和write扫描

- 非root用户不能直接读取ICMP差错报文：“端口无法到达”
- 在不具备系统管理员权限的时候可以通过使用recvfrom（）和write（）这两个系统调用来间接获得对方端口的状态
- 对远端主机的一个关闭端口第二次write调用将失败
- 在非阻塞的UDP套接字上调用recvfrom函数时，
  - 如果ICMP出错信息未收到，将返回EAGAIN（重试）错误
  - 如果ICMP出错信息到达，将返回ECONNREFUSED（连接被拒绝）错误
- Windows系统中，调用sendto函数时
  - 如果返回WSAECONNRESET，该数据包被远端主机复位
  - 如果是UDP端口，回复Port Unreachable的ICMP报文
- 通过这些区别，就可以判断出对方的端口状态如何

高级UDP扫描

- Socket API 本身提供的信息无法做出最终判断，多是利用和ICMP的组合判断
- 通过对某些特殊服务或软件的了解，向该软件监听的端口发送指定的数据
  - 端口19：基于UDP的“字符集”服务
  - 端口1434：Microsoft SQL Server服务（默认端口），发送‘\2’或者‘\3’，对方有返回值
- 这种方法有效，但是没有普遍性

慢速扫描

- 随着防火墙的广泛应用，普通的扫描很难穿过防火墙去扫描受防火墙保护的网络
- 即使扫描能穿过防火墙，扫描的行为仍然有可能会被防火墙记录下来
- 如果扫描是对非连续性端口、源地址不一致、时间间隔很长且没有规律的扫描的话，这些扫描的记录就会淹没在其他众多杂乱的日志内容中
- 使用慢速扫描的目的是：骗过防火墙和入侵检测系统而收集信息。虽然扫描所用的时间较长，但这是一种比较难以被发现的扫描

乱序扫描

- 顺序扫描
- 逆序扫描
- 乱序扫描也是一种常见的扫描技术，扫描器扫描的时候不是进行有序的扫描，扫描端口号的顺序是随机产生的，每次进行扫描的顺序都完全不一样，这种方式能有效地欺骗某些入侵检测系统而不会被发觉
  - 随机重排扫描算法：端口的顺序不被遗漏，也不重复
    - 互换位置的方式，使用一个数组和随机数产生函数
  - 线程前加延时扫描算法：不影响每个线程的创建时间
    - 每个线程中，扫描函数之前挂起一个随机时间

如何防御端口扫描

- 关闭所有不必要的端口
- 自己定期扫描网络主机、开放的端口
- 使用基于状态数据包过滤器或是代理等智能防火墙来阻塞黑客的扫描攻击

操作系统的指纹扫描(OS fingerprinting)

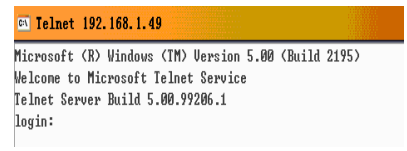
- 根据不同类型的操作系统的TCP/IP协议栈的实现特征(stack fingerprinting)来判别主机的操作系统类型，采用黑盒测试方法
- 不同的操作系统厂商的TCP/IP协议栈实现存在细微差异，对于特定的RFC文档作出不同的解释
- 向目标主机发送特殊的数据包，然后根据目标主机的返回信息在扫描工具的操作系统指纹特征数据库中查找匹配的操作系统类型

主动与被动的协议栈指纹识别

- 主动协议栈指纹识别：扫描器主动地向目标系统发送特殊格式的数据包，这种方式可能会被网络IDS系统检测出来
  - TCP包的顺序，FIN，DF，ACK序号
  - 速度快、可靠性高
- 被动协议栈指纹识别：通过被动地监听网络流量，来确定目标主机地操作系统。一般根据数据包的一些被动特征
  - 主要是TTL，窗口大小，DF，TOS
  - 被动扫描基本不具备攻击特征，有隐蔽性，依赖扫描主机所处的网络拓扑结构，速度慢、可靠性不高

扫描应用软件版本

- 在第一次连接时，许多软件都公布了版本号(如sendmail,FTP,IMAPD，Apache等)。黑客根据这些连接信息(banner)就可以知道目标的应用软件的版本信息
- 根据版本号很容易在网上查到它的已知漏洞，根据这些漏洞对目标主机进行攻击



防止网络嗅探的安全措施

- 加密
  - 远程登录——动态密码系统（One Time Password）
  - 邮件——PGP
  - SSH（RSA+IDEA）
- 网络分割
  - 网络广播的原理
  - 减小嗅探的范围

恶意软件分类

- 恶意软件是指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行，侵害用户合法权益的软件
- 可以根据多种方法对恶意软件进行分类
  - 恶意软件的行为
  - 目标平台
  - 攻击目的

根据行为进行分类

- **病毒是一段计算机代码，**可以将自身插入另一个独立程序的代码中，然后强制该程序实施恶意行为并自行传播
- **蠕虫是一种独立的恶意软件，**可以自我复制并从计算机传播到计算机。
- **木马是一个程序，**它不能自我复制，但可以伪装成用户想要的东西，并诱骗他们激活它，以便它可以实现自身的破坏和传播活动。

根据预期目的进行分类

- **间谍软件**：它会在用户使用计算机时，**窃取用户发送或接收的数据，以及监听其网络行为，并将收集到的信息发送给第三方。**其中，键盘记录程序
- **Rootkit**：在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，一般都和木马、后门等其他恶意程序结合使用
- **广告软件：**迫使浏览器重定向到网络广告，并进一步下载，甚至加载更多的恶意软件
- **勒索软件**：是近年来非常普遍的一种恶意软件形式，**主要通过加密受害者硬盘驱动器的文件，并要求支付赎金（通常为比特币等加密货币）来交换解密密钥**，如WannaCry、Petya等

远程访问木马RAT

- 远程访问木马（RAT，remote access Trojan）是一种恶意程序
  - 包括在目标计算机上用于管理控制的后门
  - 通常与用户请求的程序（如游戏程序）一起
  - 或作为电子邮件附件发送。
- 入侵者可以利用它来向其他易受感染的计算机分发远程访问木马，从而建立僵尸网络
- 远程访问木马通常包含在免费软件中，并通过电子邮件作为附件发送。

远程访问木马的危害

- 监视用户行为
- 访问机密信息，如信用卡和社会安全号码
- 激活系统的摄像头和录音录像
- 截屏
- 传播病毒和其他恶意软件
- 将驱动器格式化
- 删除、下载或改变文件和文件系统

僵尸网络Botnet

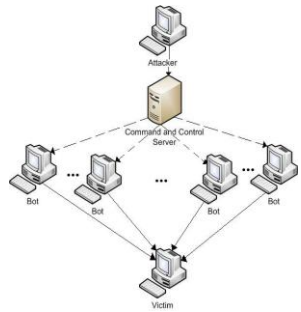
- 僵尸网络，是指采用一种或多种传播手段，将大量主机感染bot程序（僵尸程序），从而在控制者和被感染主机之间所形成的一个可一对多控制的网络。
  - “bot程序”是robot的缩写，是指实现恶意控制功能的程序代码
  - “僵尸计算机”就是被植入bot的计算机
  - “控制服务器（Control Server）”是指控制和通信的中心服务器
- 可以一对多地执行相同的恶意行为，比如可以同时对某目标网站进行分布式拒绝服务（DDos）攻击，同时发送大量的垃圾邮件等

僵尸网络的感染对象

- 巨型僵尸网络可以在任何时候对任何目标发动DDoS攻击。
- 僵尸的感染对象
  - 服务器、PC、智能手机，摄像头、路由器、家居安防系统、智能电视、智能穿戴设备等
- Mirai僵尸由于源码的开放可能正在迅速的扩散
  - 2016年10月21 日，美国知名网络域名服务提供商Dyn遭受到强力的DDoS攻击，攻击流量的来源之一是感染了Mirai僵尸的物联网IOT设备
  - IOT设备的密码固化在固件中，无法杜绝二次感染，并且隐藏在这种嵌入式设备中是极难判定其是否受到恶意感染。

分布式拒绝服务攻击（DDOS）

- 分布式拒绝服务攻击（distributed denial of service）
  - 1999年10月出现攻击
  - 1999-2000年前后，僵尸网络
    - 单一性配置，大量存在漏洞的计算机
- 僵尸网络（Bot Network）
  - 由存在不同类型漏洞的受控机器组成
  - 价值链：定向攻击，垃圾邮件，DDOS攻击
  - Fast Flux是当前的僵尸网络、恶意软件和仿冒方案最常用的通信平台



DDoS攻击分类

	停止服务	消耗资源
本地	• 杀死进程（init，inet进程） • 重新配置系统 • 使进程崩溃	• 填充进程表 • 填充整个文件系统 • 填充整个网络
远程	• 恶意数据包攻击（Land，Teardrop等）	• 数据包泛滥（SYN Flood，Smurf，DDoS等）

DDOS攻击案例：1

- SYN/ACK Flood攻击
  - 通过向受害主机发送大量伪造源IP和源端口的SYN或ACK包，导致主机的缓存资源被耗尽，由于源都是伪造的故追踪起来比较困难
  - 实施起来有一定难度，需要高带宽的僵尸主机支持
  - 少量的这种攻击会导致主机服务器无法访问，但却可以Ping通。
- 检测
  - 在服务器上用Netstat -na命令会观察到存在大量的SYN_RECEIVED状态。
- 普通防火墙大多无法抵御此种攻击。

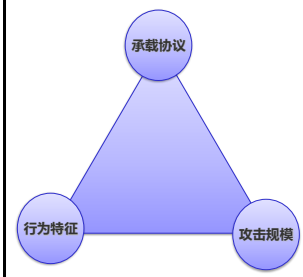
DDOS攻击案例：2

- TCP全连接攻击
  - 这种攻击是为了绕过常规防火墙的检查而设计的，一般情况下，常规防火墙大多具备过滤TearDrop、Land等DOS攻击的能力，但对于正常的TCP连接是放过的。
  - 但很多网络服务程序（如：IIS、Apache等Web服务器）能接受的TCP连接数是有限的，一旦有大量的TCP连接，即便是正常的，也会导致网站访问非常缓慢甚至无法访问。
  - TCP全连接攻击就是通过许多僵尸主机不断地与受害服务器建立大量的TCP连接，直到服务器的内存等资源被耗尽而被拖跨，从而造成拒绝服务
- 这种攻击的特点是可绕过一般防火墙的防护而达到攻击目的，缺点是需要找很多僵尸主机，并且由于僵尸主机的IP是暴露的，因此容易被追踪。

DDOS攻击案例：3

- 刷Script脚本攻击
  - 这种攻击主要是针对存在ASP、JSP、PHP、CGI等脚本程序，并调用MSSQLServer、MySQLServer、Oracle等数据库的网站系统而设计的。
  - 特征是和服务器建立正常的TCP连接，并不断的向脚本程序提交查询、列表等大量耗费数据库资源的调用。
  - 攻击者只需通过Proxy代理向主机服务器大量递交查询指令，只需数分钟就会把服务器资源消耗掉而导致拒绝服务。
- 常见的现象就是网站响应时间长、ASP程序失效、PHP连接数据库失败、数据库主程序占用CPU偏高。
  - 这种攻击的特点是可以完全绕过普通的防火墙防护，通过一些Proxy代理就可实施攻击。
  - 缺点是对付只有静态页面的网站效果会大打折扣，并且有些Proxy会暴露攻击者的IP地址。

DDoS攻击发展趋势

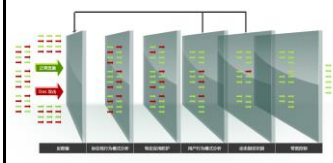


- 目标
  - 网站-》网络基础设施（路由器/交换机/DNS等）
- 流量
  - 从几兆-》几十兆-》1G甚至更高
  - 10K pps--》100K pps -》1M pps
- 技术
  - 真实IP地址-》IP欺骗技术
  - 单一攻击源-》多个攻击源
  - 简单协议承载-》复杂协议承载
  - 智能化，试图绕过IDS或FW
- 形式
  - DRDoS/ACK Flood
  - Zombie Net/BOTNET
  - Proxy Connection Flood
  - DNS Flood

常见传统缓解攻击的方法

- 轮询，负载均衡，Cache
- 路由器过滤
- 系统加固（IIS，Apache）
- SYN Cookie技术
- 借助安全设备

DDoS防御流程

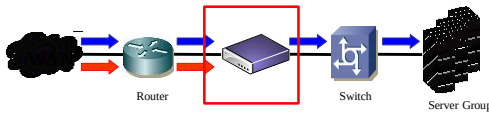


工作流程

- 智能判断是否存在攻击
  - 流量识别
  - 流量过滤
- 对不同协议的数据包采用不同处理办法
  - TCP协议
  - UDP协议
  - ICMP协议
- 对特定应用采用反向探测、自学习方法

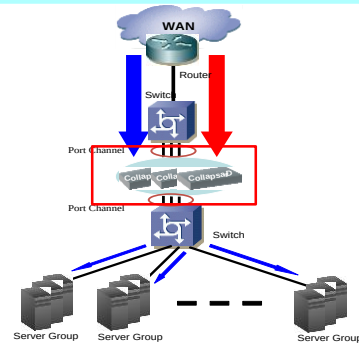
防DDoS设备应用

串联部署

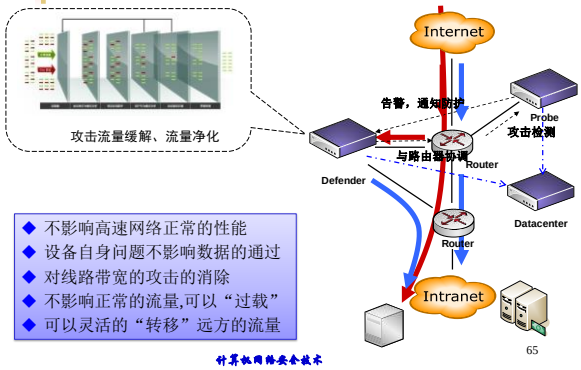


设计目标	部署要点	不足
• 少量服务器 • 小型网络 • 防火墙	• 零安装，零配置，即插即用 • 网络隐身，无IP地址配置	• 单点故障 • 网络拥塞 • 规模受限

串联集群部署



旁路部署



- ◆ 不影响高速网络正常的性能
- ◆ 设备自身问题不影响数据的通过
- ◆ 对线路带宽的攻击的消除
- ◆ 不影响正常的流量,可以“过载”
- ◆ 可以灵活的“转移”远方的流量

新型网络攻击: APT

- ◆APT高级持续性威胁(Advanced Persistent Threat)
  - ❖有组织、有特定目标、持续时间极长的新型攻击和威胁，或者称之为“针对特定目标的攻击”
  - ❖以窃取核心资料为目的，具备高度的隐蔽性，针对特定对象，长期、有计划性和组织性地窃取数据
  - ❖是以商业和政治为目的的一个网络犯罪类别
- ◆高级性主要体现在APT在发动攻击之前需要对攻击对象的业务流程和目标系统进行精确的收集。
- ◆主要特征：潜伏性，持续性，目标性，远控性

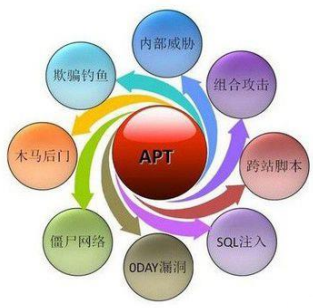
APT的主要特征

- ◆潜伏性：这些新型的攻击和威胁可能在用户环境中存在一年以上或更久
  - ❖不断收集各种信息，直到收集到重要情报。
  - ❖把“被控主机”当成跳板，持续搜索，直到能彻底掌握所针对的目标人、事、物。
- ◆持续性：由于APT攻击具有持续性甚至长达数年的特征，这让企业的管理人员无从察觉
  - ❖这种“持续性”体现在攻击者不断尝试的各种攻击手段
  - ❖渗透到网络内部后长期蛰伏。

APT的主要特征（续）

- ◆目标性：针对特定政府或企业，长期进行有计划性、组织性的窃取情报行为
  - ❖针对被锁定对象寄送社会工程恶意邮件，如冒充客户的来信,取得在计算机植入恶意软件的第一个机会。
- ◆远控性：攻击者建立一个类似僵尸网络Botnet的远程控制架构
  - ❖攻击者会定期传送有潜在价值文件的副本给命令和控制服务器(C&C Server)审查。
  - ❖将过滤后的敏感机密数据，利用加密的方式外传。

常见的APT攻击技术



APT攻击的技术特点

- ◆以智能手机、平板电脑和USB等移动设备为目标和攻击对象继而入侵企业信息系统的方式
- ◆诱骗手段
  - ❖采用恶意网站，用钓鱼的方式诱使目标上钩。而企业和组织目前的安全防御体系中对于恶意网站的识别能力还不够，缺乏权威、全面的恶意网址库，对于内部员工访问恶意网站的行为无法及时发现；
- ◆社会工程的恶意邮件
  - ❖ 攻击者也经常采用恶意邮件的方式攻击受害者，并且这些邮件都被包装成合法的发件人。而企业和组织现有的邮件过滤系统大部分就是基于垃圾邮件地址库的。另外，邮件附件中隐含的恶意代码往往都是0day漏洞，邮件内容分析也难以奏效

APT攻击的技术特点（续）

- 利用防火墙、服务器等系统漏洞继而获取访问企业网络的有效凭证信息
- SQL注入
  - 一些攻击是直接通过对目标公网网站的SQL注入方式实现的。
- 0day漏洞
  - 初始的网络渗透往往使用利用0day漏洞的恶意代码。而企业和组织目前的安全防御/检测设备无法识别这些0day漏洞攻击
- 使用SSL链接进行加密传输
  - 在攻击者控制受害机器的过程中，往往使用SSL链接，导致现有的大部分内容检测系统无法分析传输的内容
- 数据压缩加密
  - 攻击者向外部传输数据往往都是压缩、加密的，没有明显的指纹特征。这导致现有绝大部分基于特征库匹配的检测系统都失效了

APT攻击的技术特点（续）

- 缺乏知识库
  - 尽管企业部署了内网审计系统，日志分析系统等安管平台，但主要是从内控与合规的角度来分析事件，而没有真正形成对外部入侵的综合分析。由于知识库的缺乏，客户无法从多个角度综合分析安全事件，无法从攻击行为的角度进行整合，发现攻击路径。
- 缺乏防御意识
  - 攻击者往往不是直接攻击最终目标人，而是透过攻击外围人员层层渗透
- 在APT这样的新型攻击面前，大部分企业和组织的安全防御体系都失灵了

典型的APT攻击实例

- Google极光攻击
- RSA SecurID窃取攻击
- 超级工厂病毒攻击（震网攻击）
- 夜龙攻击

例1： Google极光攻击

- 2010年Google的一名雇员点击即时消息中的一条恶意链接，引发了一系列事件导致google的网络被渗入数月，并且造成各种系统的数据被窃取。
- 攻击过程：寻找特定的Google员工成为攻击者的目标
  - 搜集信息：攻击者尽可能地收集该员工在Facebook、Twitter、LinkedIn和其它社交网站上发布的信息
  - 伪造服务器：接着攻击者利用一个动态DNS供应商来建立一个托管伪造照片网站的Web服务器
  - 即时消息：利用这个伪造的web服务器，攻击者伪装成这位google员工所信任的人，并向他发送了恶意链接。

例1： Google极光攻击（续）

- Google员工点击这个未知的网络链接，就进入了恶意网站。该恶意网站页面载入含有shellcode的JavaScript程序码造成IE浏览器溢出，进而执行FTP下载程序，并从远端进一步抓了更多新的程序来执行下载。
- 窃取信息
  - 攻击者通过SSL安全隧道与受害人机器建立了连接，持续监听并最终获得了该雇员访问Google服务器的帐号密码等信息。
  - 最后，攻击者就使用该雇员的凭证成功渗透进入Google的邮件服务器，进而不断的获取特定Gmail账户的邮件内容信息。

例2：RSA SecurID窃取攻击

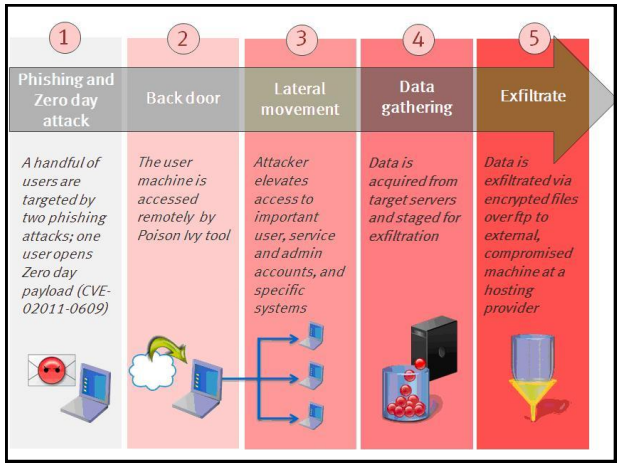
- 2011年3月，EMC公司下属的RSA公司遭受入侵，部分SecurID技术及客户资料被窃取。其后果导致很多使用SecurID作为认证凭据建立VPN网络的公司（包括洛克希德马丁公司、诺斯罗普公司等美国国防外包商）受到攻击，重要资料被窃取。
- 恶意邮件
  - 攻击者给RSA的母公司EMC的4名员工发送了两组恶意邮件
    - 邮件标题为“2011 Recruitment Plan”，寄件人是webmaster@Beyond.com，正文很简单，写着“I forward this file to you for review. Please open and view it.”；里面有个EXCEL附件名为“2011 Recruitment plan.xls”

例2：RSA SecurID窃取攻击（续）

- 其中一位员工对此邮件感到兴趣，并将其从垃圾邮件中取出来阅读。此电子表格其实含有当时最新的Adobe Flash的0day漏洞（CVE-2011-0609）。
- 该主机被植入Poison Ivy远端控制工具，并开始自BotNet的C&C服务器（位于good.mincesur.com）下载指令进行任务
- 随后，相关联的人士包括IT与非IT等服务器管理员相继被黑

例2：RSA SecurID窃取攻击（续）

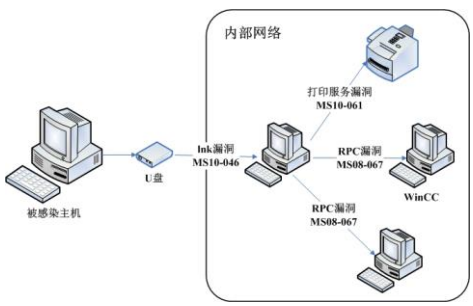
- RSA发现开发用服务器（Staging server）遭入侵，攻击方随即进行撤离，加密并压缩所有资料（rar格式），并以FTP传送至远端主机，又迅速再次搬离该主机，清除任何踪迹；
- 在拿到了SecurID的信息后，攻击者再去渗透美国最大的军火承包商的系统，窃取相应的敏感信息



例3：震网攻击

- 2010年伊朗布什尔核电站遭到Stuxnet蠕虫的攻击，导致离心机超速运转并损毁
- 核电站计算机系统实际上是与外界物理隔离的，理论上不会遭遇外界攻击。
- 超级工厂病毒的攻击者针对核电站相关工作人员的家用电脑、个人电脑等能够接触到互联网的计算机发起感染攻击，以此为第一道攻击跳板，进一步感染相关人员的U盘
- 病毒以U盘为桥梁进入“堡垒”内部，利用多种漏洞，包括当时的一个0day漏洞进行破坏。
- 有效控制攻击范围

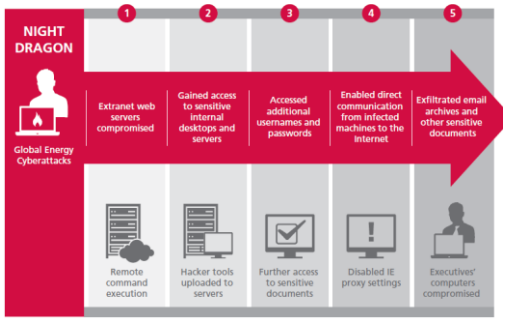
例3：震网攻击（续）



例4：夜龙攻击过程

- McAfee在2011年2月份发现并命名的针对全球主要能源公司的攻击行为。
  - 外网主机如Web服务器遭攻击成功，黑客采用的是SQL注入攻击
  - 被黑的Web服务器被作为跳板，对内网的其他服务器或PC进行扫描；
  - 内网机器如AD服务器或开发人员电脑遭攻击成功，可能是被密码暴力破解；
  - 被黑机器被植入恶意代码，并被安装远端控制工具（RAT），并禁用掉被黑机器IE的代理设置，建立起直连的通道，传回大量文件（WORD、PPT、PDF等等），包括所有会议记录与组织人事架构图；
  - 更多内网机器遭入侵成功，多半为高阶主管点击了看似正常的邮件附件，却不知其中含有恶意代码

例4：夜龙攻击过程



社会工程学（Social Engineering）

- 社会工程学是信息网络安全中的一个新的分支，其主要特点就是利用人的弱点来进行攻击
- 社会工程学
  - 是把对物的研究方法全盘运用到对人本身的研究上，并将其变成技术控制的工具。
  - 社会工程学是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的方法。
- 结合网络安全中的最新技术进行攻击，尤其结合浏览器等应用程序漏洞来进行钓鱼攻击等，危害巨大

生活中的社会工程学攻击

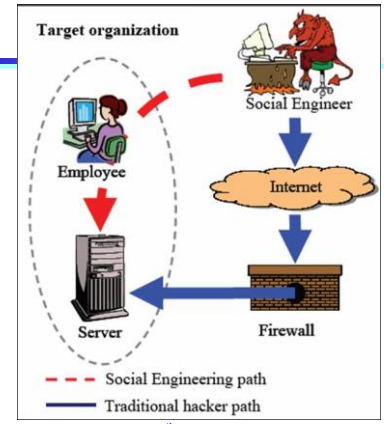
- 环境渗透
- 身份伪造
- 冒名电话
- 信件伪造
- 个体配合
- 反向社会工程学
  - 迫使目标人员反过来向攻击者求助的手段

网络中的社会工程学攻击

- 地址欺骗
  - 钓鱼技术 (Phishing)：模仿合法站点的非法站点，利用欺骗性的电子邮件或者跨站攻击诱导用户前往伪装站点，目的是截获受害者输入的个人信息（比如密码）
  - 域欺骗：钓鱼技术+ DNS 缓冲区毒害技术 (DNS caching poisoning)：攻击 DNS 服务器，将合法 URL 解析成攻击者伪造的 IP 地址； 在伪造 IP 地址上利用伪造站点获得用户输入信息
- 邮件欺骗
  - 木马植入：在欺骗性信件内加入木马或病毒
  - 群发诱导：欺骗接收者将邮件群发给所有朋友和同事

网络中的社会工程学攻击（续）

- 非交互式技术
  - 不通过和目标人员交互即可获得所需信息技术
  - 利用合法手段获得目标人员信息，如利用搜索引擎获得个人信息，包括地址、电话号码等
  - 利用非法手段在薄弱站点获得安全站点的人员信息
- 多学科交叉技术
  - 心理学技术：分析网管的心理以利用于获得信息
    - 常见配置疏漏：明文密码本地存储、便于管理简化登陆
    - 安全心理盲区：容易忽视本地和内网安全、对安全技术（比如防火墙、入侵检测系统、杀毒软件等）盲目信任、信任过度传递
  - 组织行为学技术：分析目标组织的常见行为模式，为社会工程提供解决方案。



无线网络安全

补充

无线网络的安全事件

- 公共免费Wi-Fi安全隐患
  - 利用伪造的Wi-Fi热点，不法分子可以在几分钟之内获得上网用户的设备运行数据、网络账户、密码、照片等私密信息，甚至可以窃取用户网银资产
- 非法AP：未经企业许可而私自接入企业网络中的无线路由器Rogue AP
- 家用无线路由器的安全问题
  - 一些路由器厂家为了日后调试和检测更方便，会在产品上保留超级管理权限。黑客可以利用这些后门直接控制路由器，进一步发起DNS劫持、窃取信息、网络钓鱼等攻击
  - 通过HTTP和SSH默认端口远程访问，恶意软件的变种被注入路由器
  - 密码破解
    - 无线路由器的接入密码和后台密码
    - 。。。

无线网络的特点

- 信道
  - 共享，易受到监听和干扰
- 移动性
  - 移动性带来的安全隐患
- 资源
  - 移动设备中操作系统复杂，存储空间和资源有限
- 可访问性
  - 一些无线设备无人值守，易受到物理攻击

大作业提交通知

- 小组提交的作业（6月10日 20:00之前）
  - 每个小组提交程序和ppt（打包成rar或zip格式）
    （1）提交一份程序和数据，程序加注释和运行环境说明。
    （2）每组完成一份ppt（讲10分钟左右）。

6月12日课上大作业检查

- 每人提交技术报告（6月16日 20:00之前）
  - 每位同学根据大作业承担的工作独立完成并提交大作业技术报告。
  - 格式参考期刊论文要求，篇幅不限。